

①⑨ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENT- UND
MARKENAMT

⑫ Patentschrift
⑩ DE 40 04 709 C 2

GB 2 241 361

- ⑳ Aktenzeichen: P 40 04 709.1-53
㉑ Anmeldetag: 15. 2. 90
㉒ Offenlegungstag: 22. 8. 91
㉓ Veröffentlichungstag
der Patenterteilung: 7. 1. 99

⑤⑦ Int. Cl. 6:
G 06 F 9/445
G 06 F 11/00
G 06 F 1/24

DE 40 04 709 C 2

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

⑬ Patentinhaber:
Robert Bosch GmbH, 70469 Stuttgart, DE

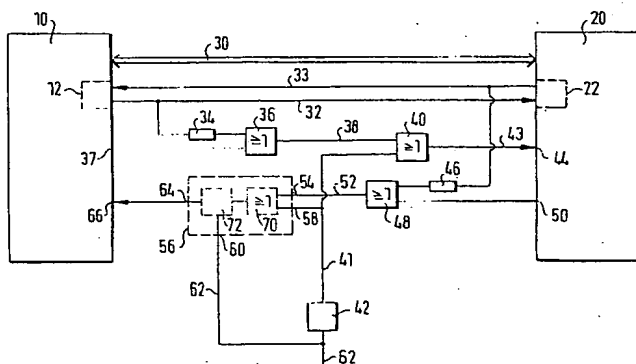
⑰ Erfinder:
Preis, Karl-Heinrich, Dipl.-Ing., 77830 Bühlertal, DE

⑤⑥ Für die Beurteilung der Patentfähigkeit in Betracht
gezogene Druckschriften:

DE 37 90 885 A1
DE 37 26 489 A1
US 42 34 926

⑤④ Rechnersystem

⑤⑦ Rechnersystem mit wenigstens zwei Recheneinheiten, die über wenigstens ein Leitungssystem zum Austausch von Daten und/oder Steuer- bzw. Kontrollsignalen verbunden sind und bei Inbetriebnahme durch ein auf beide wirkendes Rücksetzsignal initialisiert werden (power-on-reset), wobei das Rechnersystem mit wenigstens einem Mittel zur Erkennung von fehlerhaften Zuständen der Recheneinheiten ausgestattet ist (Watch-Dog, Datenaustauschprotokoll) und bei fehlerhaften Zuständen einer der Recheneinheiten diese durch ein nur auf sie wirkendes Rücksetzsignal erneut in Betrieb genommen wird (Reset), dadurch gekennzeichnet, daß das Rechnersystem mit einer zusätzlichen signalerzeugenden Einheit ausgestattet ist, die bei Inbetriebnahme des Rechnersystems wenigstens eine der Recheneinheiten durch einen vom initialisierenden Rücksetzsignal unabhängigen Rücksetzimpuls initialisiert.



DE 40 04 709 C 2

Beschreibung

Die Erfindung betrifft ein Rechnersystem gemäß dem Oberbegriff des Patentanspruchs 1.

Ein derartiges Rechnersystem zur Steuerung eines Betriebsparameters einer Brennkraftmaschine eines Kraftfahrzeugs ist aus der DE 37 26 489 A1 bekannt. Dort ist ein Rechnersystem bestehend aus zwei Prozessoren, die über ein Leitungssystem zum Austausch von Daten und Steuer- bzw. Kontrollsignalen verbunden sind, vorgeschlagen. Zur gegenseitigen Überwachung der beiden Prozessoren ist jeder Prozessor mit einem sogenannten Watch-Dog ausgestattet, der an den jeweils anderen Rechner Kontrollsignale abgibt, anhand derer der jeweils andere Rechner die Funktionsfähigkeit des das Kontrollsignal aussendenden Rechners überprüfen kann. Ein zweiter Überwachungspfad wird bei einem derartigen Zwei-Rechner-System durch die Übertragung von Daten zwischen den beiden Prozessoren aufgebaut. Die Datenübertragung erfolgt zyklisch in einem festen Zeitraster, bei Ausbleiben einer Datenübertragung bzw. -anforderung eines der beiden Rechner schließt der jeweils andere auf einen Funktionsfehler und startet den fehlerhaften Rechner über einen Reset-Impuls neu (Warmstart). Bei Inbetriebnahme des Rechnersystems wird ein beiden Rechnern gemeinsamer Initialisierungsimpuls (Power on) erzeugt, der beide Rechner gleichzeitig zur Initialisierung zurücksetzt (Kaltstart). Nachteilig an einer derartigen Anordnung ist, daß das Rechnersystem nicht ordnungsgemäß im Betrieb genommen werden kann, wenn der Initialisierungsimpuls bzw. die diesen Impuls erzeugende Schaltungsanordnung fehlerbehaftet ist. Dient das Rechnersystem zur Steuerung sicherheitskritischer Funktionen einer Brennkraftmaschine und/oder eines Kraftfahrzeugs, besteht die Gefahr, daß in einem derartigen Fehlerfall ein sicherheitskritischer Fahrzustand auftreten kann.

Der Erfindung liegt daher die Aufgabe zugrunde, die Verfügbarkeit eines derartigen Rechnersystems zu verbessern. Dazu ist eine zusätzliche Einheit vorgesehen, die einen vom eigentlichen Initialisierungsimpuls unabhängigen zweiten Initialisierungsimpuls erzeugt.

Aus dem US-Patent 4,234,926 ist es bekannt, bei einem Computer zusätzlich zu und unabhängig von einem Rücksetzsignal einen durch eine zusätzliche signalerzeugende Einheit (external reset switch) erzeugten Rücksetzimpuls vorzusehen.

Aus der DE 37 90 885 A1 ist eine Schaltungsanordnung zur Erzeugung eines Initialisierungs- bzw. Rücksetzimpuls beschrieben. Diese Schaltungsanordnung dient einerseits zum Rücksetzen eines Rechnersystems beim ersten Einschalten (Power on), andererseits zum Rücksetzen des Rechnersystems bei Unterspannung, d. h. bei Absinken der Betriebsspannung unter einen vorgegebenen Wert. Ferner erzeugt diese vorgeschlagene Schaltungsanordnung ein Rücksetzsignal, das bei einem Ausfall eines Rechners von einem funktionsfähigen Rechner ausgelöst wird, um den funktionsunfähigen Rechner neu zu starten.

Vorteile der Erfindung

Die Erfindung hat den Vorteil, daß bei Ausfall der den Initialisierungs- bzw. Rücksetzimpuls erzeugenden Schaltungsanordnung eine ordnungsgemäße Inbetriebnahme des Rechnersystems durch eine zusätzliche, von dieser Schaltungsanordnung unabhängige Einheit ermöglicht wird. Eine fehlerhafte Inbetriebnahme und ein daraus folgender sicherheitskritischer Zustand kann dadurch wirksam vermieden werden.

In Verbindung mit aus dem Stand der Technik bekannten

Überwachungsverfahren eines derartigen Rechnersystems kann die zusätzliche Einheit auf einfache, kostengünstige Art realisiert werden.

Weitere Vorteile der Erfindung ergeben sich aus den Unteransprüchen in Verbindung mit dem im folgenden beschriebenen Ausführungsbeispiel.

Zeichnung

Im folgenden wird die Erfindung anhand des in der Zeichnung dargestellten Ausführungsbeispiels erläutert. Fig. 1 zeigt ein Beispiel eines als Blockschaltbild dargestellten Zwei-Rechner-Systems mit zusätzlicher Rücksetzeinheit, Fig. 2 ein Übersichtsflußdiagramm des Zusammenspiels von Rechnerüberwachung und zusätzlicher Rücksetzeinheit bei der Inbetriebnahme des Rechnersystems. Fig. 3 schließlich stellt eine schaltungstechnisch einfache, kostengünstige Realisierungsform der zusätzlichen Rücksetzeinheit vor.

Beschreibung eines Ausführungsbeispiels

Fig. 1 zeigt beispielhaft ein Zwei-Rechner-System, das zur Ausführung bestimmter Funktionen im Kraftfahrzeug dient. Beispielsweise können derartige Zwei-Rechner-Systeme bei Sicherheitseinrichtungen wie Airbag oder Gurtstraffer eingesetzt werden, oder zur Steuerung und/oder Regelung von Betriebsparametern der Brennkraftmaschine eines Kraftfahrzeugs, beispielsweise in einer elektronischen Motorleistungssteuerung, angewendet werden.

Die beiden Recheneinheiten 10 und 20 sind über ein Leitungssystem 30 verbunden. Ein derartiges Leitungssystem kann Datenleitungen, Adressleitungen und/oder Steuerleitungen umfassen. Das Leitungssystem 30 dient zum Austausch von Daten, Adressen und/oder Steuer- oder Kontrollsignalen, mit deren Hilfe die Kommunikation zwischen den beiden Rechnern gesteuert wird. Beide Recheneinheiten 10 und 20 sind mit sogenannten Watch-Dogs 12, 22 ausgestattet. Die beiden Watch-Dog-Einheiten sind über zwei Leitungen 32, 33 miteinander verbunden, wobei die Leitung 32 das von der Watch-Dog-Einheit 12 erzeugte Signal führt, die Leitung 33 das von der Watch-Dog-Einheit 22 erzeugte.

Die Verbindungsleitung 32 ist ferner über eine Schaltungseinheit 34 auf einen Eingang einer Verknüpfungsstufe 36 geführt. Diese Verknüpfungsstufe 36, die einer logischen ODER-Funktion entspricht, ist an ihrem zweiten Eingang mit einem Ausgang 37 der Recheneinheit 10 verbunden. Die Ausgangsleitung 38 der Verknüpfungsstufe 36 bildet die Eingangsleitung einer zweiten Verknüpfungsstufe 40, deren zweiter Eingang über eine Leitung 41 mit einer Schaltungsanordnung 42 zur Bildung eines Rücksetzimpulses bzw. Initialisierungsimpulses verknüpft ist. Die Ausgangsleitung 43 der ebenfalls eine logische ODER-Funktion ausführenden Verknüpfungsstufe 40 ist auf den Eingang 44 der Recheneinheit 20 geführt.

In analoger Weise ist die Verbindungsleitung 33 über eine Schaltungseinheit 46 mit einer dritten Verknüpfungsstufe 48 verbunden, deren zweiter Eingang mit einem Ausgang 50 der Recheneinheit 20 verknüpft ist. Die Ausgangsleitung 52 der Verknüpfungsstufe 48 wird auf den Eingang 54 einer Einheit 56 zur Bildung eines unabhängigen Rücksetzimpulses geführt. Die Einheit 56 ist an einem weiteren Eingang 58 mit der Einheit 42 zur Bildung eines Rücksetz- bzw. Initialisierungsimpulses über die Leitung 41 verbunden. Ein dritter Eingang 60 der Einheit 56 ist mit der Leitung 62 beaufschlagt, die gleichzeitig die Eingangsleitung der Einheit 42 bildet und die Versorgungsspannung des Systems führt. Der Ausgang 64 der Einheit 56 ist schließlich mit dem Eingang 66 der Recheneinheit 10 verbunden.

Die Funktionsweise des in Fig. 1 dargestellten Systems ergibt sich aus dem folgenden. Die Einheit 42 bildet in Abhängigkeit des über die Leitung 62 ihr zugeführten Versorgungsspannungswertes ein Impulssignal, welches über die Leitung 41 die Verknüpfungsstufe 40 und die Leitung 43 den Rechner 20 über dessen Reset-Eingang 44 zurücksetzt. Ein derartiger Rücksetzimpuls tritt beispielsweise bei Inbetriebnahme des Systems als Initialisierungsimpuls auf. Der Rücksetzimpuls ist ferner über den Eingang 58 der Einheit 56 und die Ausgangsleitung 64 der Einheit 56 auf den Reset-Eingang 66 der Recheneinheit 10 geführt. Die Recheneinheit 10 wird gleichzeitig mit der Recheneinheit 20 bei der oben beschriebenen Betriebsbedingung gestartet. Im ausgeführten Beispiel werden vorzugsweise die Rechner durch ein positives "high"-Signal zurückgesetzt. Im Initialisierungsfall führen die Ausgänge 12, 37 bzw. 22, 50 "low"-Potential.

Die gegenseitige Funktionsüberwachung der beiden Rechner wird entsprechend der eingangs genannten DE 37 26 489 A1 durchgeführt. Ein erster Überwachungspfad ist dabei im zyklischen, im festen Zeitraster betriebenen Datenaustausch zu sehen. Eine der Recheneinheiten 10 oder 20 erwartet dabei in einem festen Zeitraster eine Datenanforderung der jeweilig anderen über das Leitungssystem 30. Die die Datenanforderung aussprechende Recheneinheit erwartet daraufhin eine Datenübertragung der jeweilig anderen. Bleibt eine dieser Reaktionen aus, wird die jeweilige Recheneinheit als fehlerhaft erkannt. Die funktionstüchtige Recheneinheit startet dabei über ihren Restart-Ausgang (im Falle der Recheneinheit 10 der Ausgang 37, im Fall der Recheneinheit 20 über den Ausgang 50) die fehlerhafte neu. Die jeweilige Recheneinheit sendet dabei im Falle einer Fehlfunktion der Recheneinheit 20 einen Rücksetzimpuls über die Verknüpfungsstufen 36 und 40 zu dem Reset-Eingang 44, für den Fall, daß die Recheneinheit 10 eine Fehlfunktion zeigt über die Verknüpfungsstufe 48 und die Einheit 56 auf den Reset-Eingang 66 der Recheneinheit 10. Der erfolgreiche Neustart der fehlerhaften Recheneinheit kann anhand des oben beschriebenen Datenprotokolls oder anhand der im folgenden beschriebenen Watch-Dog-Überwachung durchgeführt werden.

Ein weiterer Überwachungspfad ist durch den gegenseitigen Austausch von Watch-Dog-Kontrollsignalen zwischen den beiden Recheneinheiten gegeben. Dabei wird von der Watch-Dog-Einheit 12 ein Kontrollsignal über die Leitung 32 an die Watch-Dog-Einheit 22 der Recheneinheit 20 abgegeben, die dieses auswertet und anhand der Signalform und/oder Höhe die Funktionstüchtigkeit der Recheneinheit 10 bestimmt. Analog wird ein ähnliches Kontrollsignal von der Einheit 22 über die Leitung 33 an die Watch-Dog-Einheit 12 der Recheneinheit 10 übermittelt und dort ausgewertet. Die Leitungen 32 und 33 sind mit Schaltungseinheiten 34 bzw. 46 verbunden, die das Kontrollsignal auswerten und im Falle eines Fehlers einen Rücksetzimpuls über die Verknüpfungsstufen 36 und 40 an den Rücksetzeingang 44 der Recheneinheit 20 im Falle des Ausfalls der Recheneinheit 10 und über die Verknüpfungsleitung 48 und die Einheit 56 an den Rücksetzeingang 66 der Recheneinheit 10 im Fehlerfall der Recheneinheit 20 zuführen, wobei darauffolgend die jeweils fehlerhafte Recheneinheit von der anderen neu gestartet wird. Die Verknüpfungsstufen 36, 40 und 48 sind dabei als logische ODER-Verknüpfung ausgebildet, um eine Gleichberechtigung der Rücksetzimpulse der Einheit 42, aufgrund eines fehlerhaften Watch-Dog-Signales oder aufgrund eines Neustartsignals zu erreichen.

Die Einheit 56, von der ein Realisierungsbeispiel in Fig. 3 beschrieben ist, besteht im wesentlichen aus einer logischen ODER-Verknüpfung 70, die eine Gleichberechtigung zwi-

schen dem am Eingang 54 der Einheit 56 über die Verbindungsleitung 52 von der Verknüpfungsstufe 48 gelieferten Rücksetzsignalen mit dem im fehlerfreien Zustand von der Einheit 42 über Leitung 41 an den Eingang 58 der Einheit 56 zugeführten Rücksetzsignal gewährleistet. Ferner ist eine impulsbildende Stufe 72 Bestandteil der Einheit 56. Dieser impulsbildenden Stufe 72 ist der Ausgang der logischen ODER-Verknüpfung 70 und ein Versorgungsspannungssignal über die Verbindungsleitung 62 und den Eingang 60 der Einheit 56 zugeführt, wobei der Ausgang der impulsbildenden Stufe 72 mit dem Ausgang 64 der Einheit 56 verbunden ist und den Reset-Eingang 66 der Recheneinheit 10 bedient.

Die impulsbildende Stufe 72 kann in einem bevorzugten Ausführungsbeispiel als differenzierendes Element ausgeführt sein. Fällt die Einheit 42 zur Bildung eines Rücksetzsignales bei Inbetriebnahme aus, so dient die impulserzeugende Einheit 72 zur Bildung eines Rücksetzsignals aus dem über die Leitung 62 zugeführten Versorgungsspannungssignal. Die Stufe 72 liefert bei Inbetriebnahme des Systems einen Rücksetzimpuls an den Reset-Eingang 66 der Recheneinheit 10, der diese initialisiert und startet. Anhand der oben beschriebenen Überwachungspfade kann die Recheneinheit 10 eine Fehlfunktion der Einheit 20 erkennen und diese neu starten, indem sie über ihren Ausgang 37 bei erkannter Fehlfunktion der Einheit 20 deren Reset-Eingang 44 ein Rücksetzsignal zuführt. Dadurch ist auch bei Ausfall der Einheit 42 eine ordnungsgemäße Inbetriebnahme des Systems gewährleistet.

Der erfindungsgemäße Gedanke ist auch auf Mehrrechnersysteme anwendbar, ferner ist es auch möglich, daß die Einheit 56 der Recheneinheit 20 zugeordnet ist.

In Fig. 2 wird der erfindungsgemäße Gedanke anhand eines Übersichtsflußdiagramms dargestellt, das in prinzipieller Weise den Ablauf bei Inbetriebnahme des Rechnersystems in der Recheneinheit, der die Einheit 56 zugeordnet ist, beschreibt. Im Schritt 100 wird bei Inbetriebnahme des Rechnersystems die jeweilige Recheneinheit durch Rücksetzimpulse initialisiert. Im fehlerfreien Betriebsfall geschieht dies durch den von der Einheit 42 gelieferten Initialisierungsimpuls. Ist diese defekt, so liefert die Einheit 56 einen zusätzlichen Impuls an die ihr zugeordnete Recheneinheit. Im Abfrageblock 102 wird die Funktionstüchtigkeit der im Zwei-Rechner-System zweiten Recheneinheit, der die Einheit 56 nicht zugeordnet ist, überprüft. Ist dies der Fall, so kann geschlossen werden, daß eine ordnungsgemäße Inbetriebnahme stattgefunden hat und in Block 110 der Normalbetrieb des Rechnersystems festgestellt. Arbeitet die andere Recheneinheit jedoch fehlerhaft, so wird entsprechend Block 104 diese von der ordnungsgemäß gestarteten Recheneinheit zurückgesetzt. Im Schritt 106 wird dann die ordnungsgemäße Arbeitsweise der neu gestarteten Recheneinheit überprüft, im Falle einer ordnungsgemäßen Arbeitsweise ein ordnungsgemäßer Start des Systems festgestellt (110), arbeitet die neugestartete Recheneinheit dennoch fehlerhaft, so wird im Schritt 108 diese Recheneinheit als fehlerhaft erkannt und abgeschaltet.

Fig. 3 zeigt eine schaltungstechnische Realisierungsform der Einheit 56. Die in Fig. 1 verwendeten Bezugszeichen der Ein- bzw. Ausgänge der Einheit 56 sind dabei beibehalten worden. Eine einfache, kostengünstige Realisierungsmöglichkeit besteht aus zwei Dioden, einem Widerstand und einem Kondensator.

Der Eingang 54, an dem gegebenenfalls das aufgrund eines fehlerhaften Watch-Dog-Signals oder eines Neustartsignals des jeweilig anderen Rechners anliegt, ist auf die Anode einer Diode 200 geführt. Deren Kathode ist mit einem Verknüpfungspunkt 202 verknüpft. Der Eingang 58, an dem gegebenenfalls der Initialisierungs- bzw. Rücksetzimpuls

der Einheit 42 anliegt, ist auf die Anode einer zweiten Diode 204 geführt, deren Kathode ebenfalls mit dem Verknüpfungspunkt 202 verbunden ist. Die beiden Dioden bilden dabei die weiter oben beschriebene logische ODER-Verknüpfung, wobei die beiden an den Eingängen 54 und 58 anliegenden Signale gleichberechtigt an den Ausgang 64, der direkt mit dem Verknüpfungspunkt 202 verbunden ist, weitergegeben werden. Am Verknüpfungspunkt 202 ist ferner ein Kondensator angeschlossen, der andererseits mit dem Eingang 60 der Einheit 56 verbunden ist. Den Verknüpfungspunkt 202 verbindet ein Widerstand 208 mit Masse.

Bei Inbetriebnahme des Rechnersystems liegt am Eingang 60 der Einheit 56 ein entsprechendes Spannungssignal an. Der Kondensator 206 wird entsprechend der Veränderung des Spannungssignals aufgeladen, so daß die Kondensatorspannung exponentiellen Verlauf annimmt. Die zeitliche Veränderung der Kondensatorspannung führt zu einer entsprechenden, inversen zeitlichen Veränderung des Potentialverlaufs am Verknüpfungspunkt 202. Dieser Potentialverlauf stellt ein impulsförmiges "high"-Signal mit einer steilen und einer entsprechend dem ansteigenden Verlauf der Kondensatorspannung abfallenden Flanke dar. Das auf diese Weise gebildete Impulssignal liegt am Ausgang 64 der Einheit 56 an und wird dem Reset-Eingang der zugeordneten Recheneinheit zugeführt, worauf diese zurückgesetzt wird. Auf diese Weise ist unabhängig vom Signal der Einheit 42 ein ordnungsgemäßer Start des Rechnersystems gewährleistet.

Die erfindungsgemäße Vorgehensweise kann prinzipiell auch bei Unterspannungen Anwendung finden.

Patentansprüche

1. Rechnersystem mit wenigstens zwei Recheneinheiten, die über wenigstens ein Leitungssystem zum Austausch von Daten und/oder Steuer- bzw. Kontrollsignalen verbunden sind und bei Inbetriebnahme durch ein auf beide wirkendes Rücksetzsignal initialisiert werden (power-on-reset), wobei das Rechnersystem mit wenigstens einem Mittel zur Erkennung von fehlerhaften Zuständen der Recheneinheiten ausgestattet ist (Watch-Dog, Datenaustauschprotokoll) und bei fehlerhaften Zuständen einer der Recheneinheiten diese durch ein nur auf sie wirkendes Rücksetzsignal erneut in Betrieb genommen wird (Restart), **dadurch gekennzeichnet**, daß das Rechnersystem mit einer zusätzlichen signalerzeugenden Einheit ausgestattet ist, die bei Inbetriebnahme des Rechnersystems wenigstens eine der Recheneinheiten durch einen vom initialisierenden Rücksetzsignal unabhängigen Rücksetzimpuls initialisiert.
2. Rechnersystem nach Anspruch 1, dadurch gekennzeichnet, daß die vom zusätzlichen Rücksetzsignal beaufschlagte Recheneinheit ein fehlerhaftes Arbeiten der anderen erkennt und diese bei erkanntem fehlerhaften Arbeiten neu startet.
3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die zusätzliche Einheit im wesentlichen aus einem differenzierenden Element, vorzugsweise einem RC-Element, besteht.

Hierzu 2 Seite(n) Zeichnungen

FIG. 1

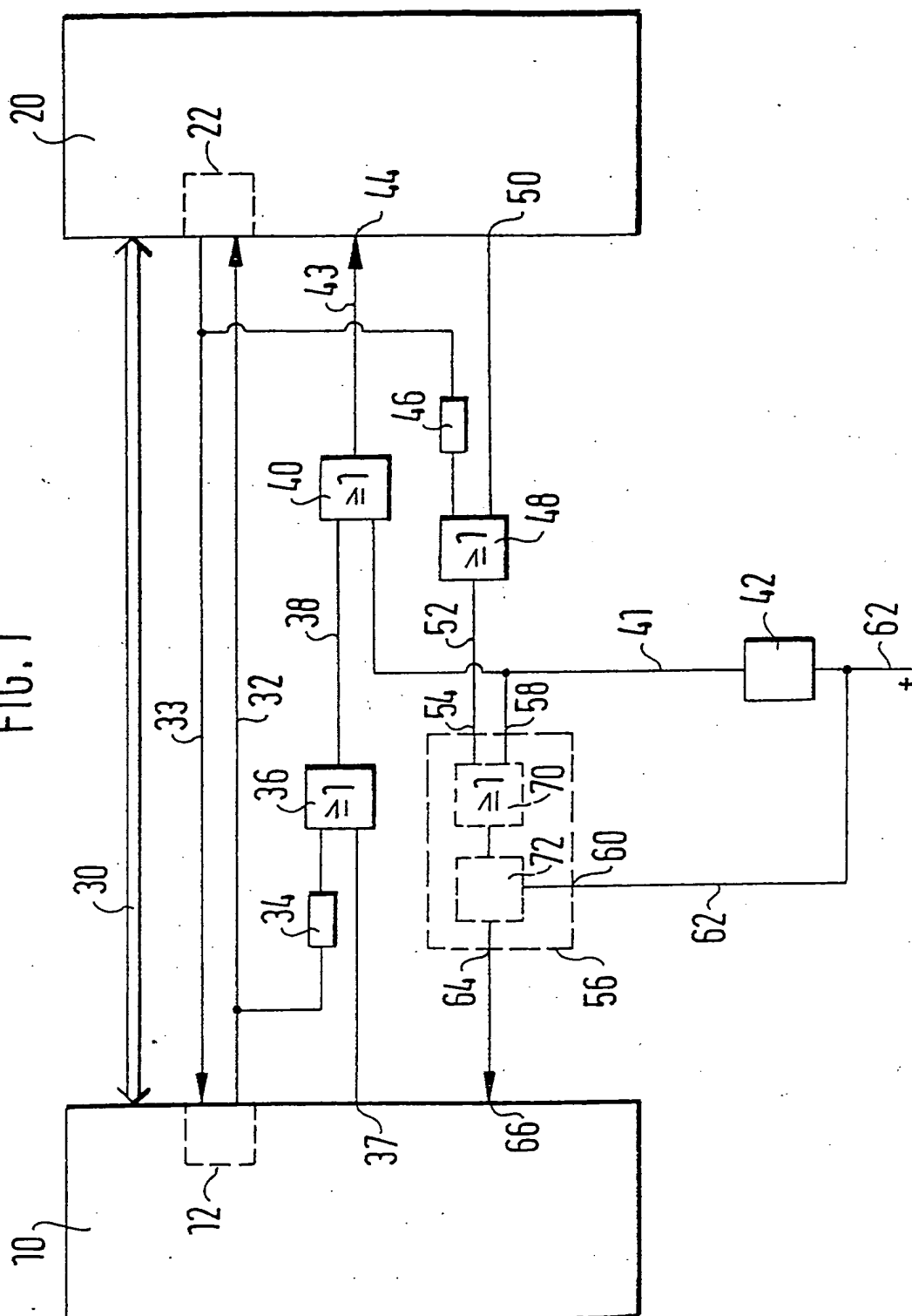


FIG. 2

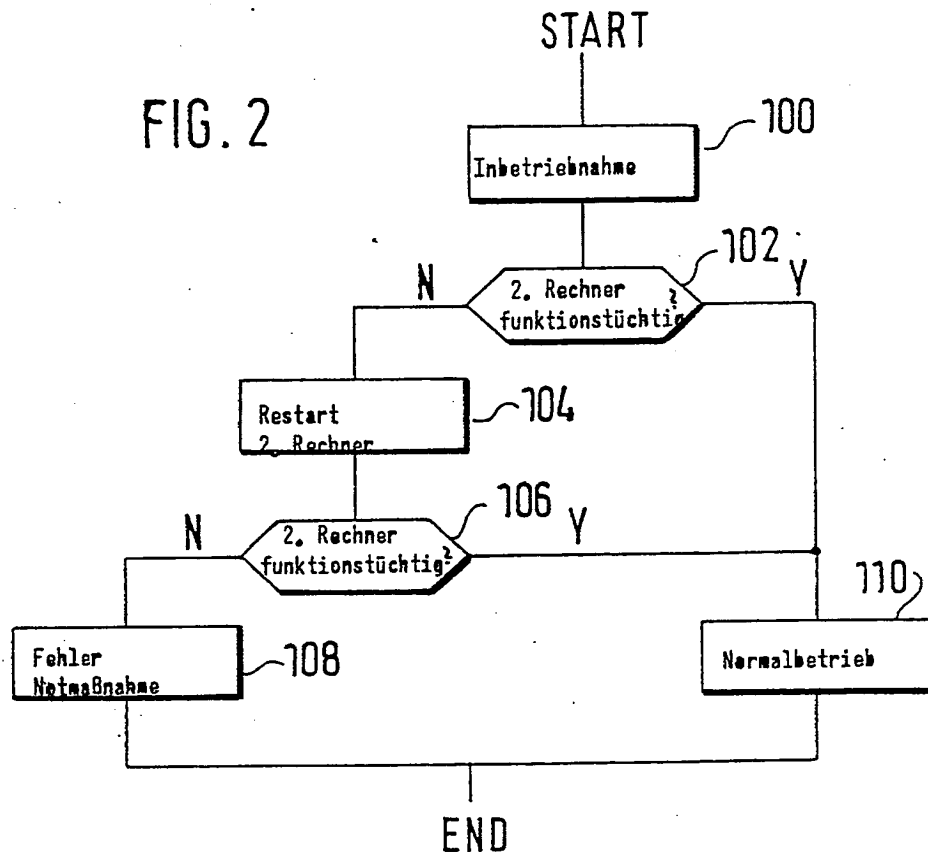
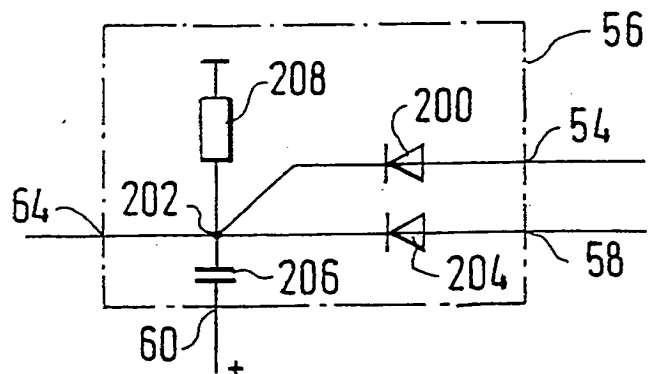
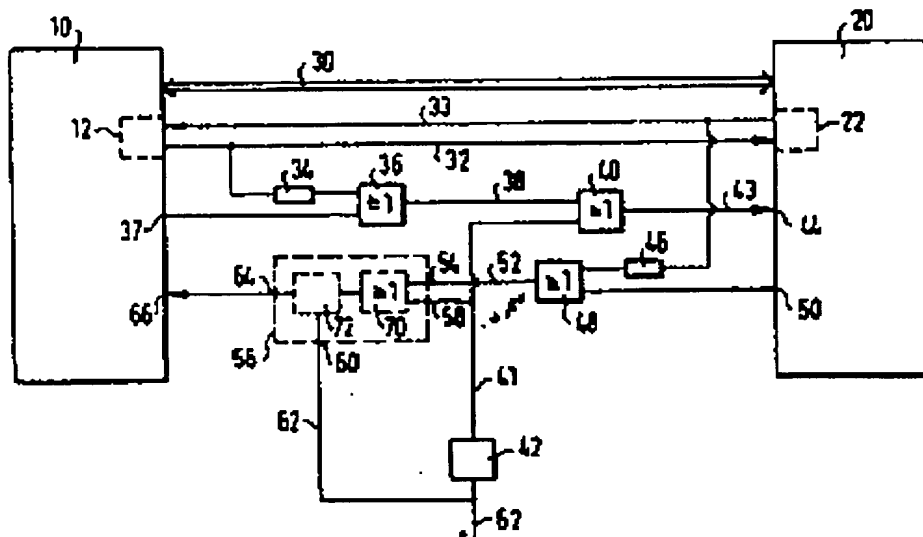


FIG. 3



AN: PAT 1991-25334
TI: Computer system, e.g. for vehicle IC engine parameter control has additional pulse generator enabling orderly start-up
PN: DE4004709-A
PD: 22.08.1991
AB: The computer system has at least two computer units connected via a cable system for exchanging data and/or control and monitoring signals and is initialised by a reset signal when powered up. The system detects computer fault states and restarts a computer unit when a fault state is detected. An additional signal generating unit supplies a reset pulse independent of the initialising signal to at least one computer unit at power-on.;
PA: (BOSC) BOSCH GMBH ROBERT;
IN: PREIS K H; PREIS K; PRIES K;
FA: DE4004709-A 22.08.1991; JP3217077-B2 09.10.2001;
GB2241361-A 28.08.1991; FR2658335-A 16.08.1991;
GB2241361-B 11.08.1993; DE4004709-C2 07.01.1999;
CO: DE; FR; GB; JP;
IC: B62D-006/00; G06F-001/24; G06F-009/44; G06F-009/445; G06F-011/00; G06F-011/14; G06F-011/18; G06F-011/30; G06F-015/16; G06F-015/177;
MC: T01-F05; T01-G09; T01-J02; X22-A03;
DC: Q22; T01; X22;
FN: 1991253347.gif
PR: DE4004709 15.02.1990;
FP: 16.08.1991
UP: 02.11.2001



THIS PAGE BLANK (USPTO)

DOCKET NO: S3-02P14830

SERIAL NO: 10/535,126

APPLICANT: Grafhoff et al.

LEARNER AND GREENBERG P.A.

P.O. BOX 2480

HOLLYWOOD, FLORIDA 33022

TEL. (954) 925-1100